CYBER CRIMES DURING COVID - 19 PANDEMIC

DR. SOMLATA SHARMA
Assistant Professor MDU – CPAS Gurugram (HR)
Email- sharma.shamli@gmail.com

SHOBHA YADAV
Research Scholar MDU – CPAS Gurugram (Haryana)
Email - adv.shobhayadav@gmail.com

ABSTRACT

With the growth of new technology and the advent of mode of communication , internet has become a new form of life. In todays age, information technology is very important technology which is used almost all types of organizations. Due to covid 19 pendamic, cyber crime increasing very fast. An offender of cyber can easily hacked or destroyed any websites or portal or spreading viruses. Covid -19 is infected disease which caused coronavirus. As business, government agencies and human being are also rely on it. Today, we are living in this world where all work is done in a digital form. Its also affects our e-life. In this current e-age, crime is happened beyond the physical assault as well as mental torture. Nowadays, its an illegal activities. From this research paper, researcher wants to highlights problem on cyber crimes during covid 19 pandemic , range of cyber attack during coronavirus and lockdown measures to prevent the spread of the virus. Because misuse of digital technology for the criminal activities is increasing day to day which is result of cyber crime .

Keywords : *Cyber crime, Covid 19, Information technology, Internet, Coronovirus*

INTRODUCTION

Covid – 19 is causing very harmful for millions of people. Every people are relying on computer system, mobile devices and internet to work or communicate, share and received data. But otherwise it mitigate the impact of social distancing. This period of social distancing and misinformation also gave an opportunity to the dark elements of the society. Cyber crime and Covid has been a deluge of phony or fake applications, domain names and sites gaining by two realities, first, the dread among the overall population and their quest for data identified with this pandemic and besides, the organizations across the globe are diverting to 'telecommute' by means of the online medium. We will manage both the situations individually. Online traffics escalated from the video conference, meeting, online classes and chatting etc. The use of apps like Paytm, Google Pay, BHIM, Phonepe, etc. as a mode of making payments has also witnessed a surge. Online fraud are growing very fast.

During the lockdown, digital hoodlums received new ways. "Individuals made phony government sites giving positions to specialists and attendants for Covid patients. Then, at that point there were individuals selling sanitisers, PPE units and food on counterfeit sites… Some programmers additionally accessed ledgers with KYC stages… The QR code cheating through an online affiliate site got renowned," Cyber offenders have been caught up with abusing weaknesses. Year 2020 saw perhaps the biggest number of information breaks and the numbers appear to be just rising. The total number of attacks recorded in India during Jan & Feb 2021 was around 15 million.

In march , 2020, Government imposed curfew for prevention of coronavirus. Then every work was done from working from homes through the video conferences and conference calls. Increasing internet and working from home created digital security risk. It also gives an opportunity to the cyber criminals for the cyber attacks. That was spreading high peak data traffics . Home networks are less secured and private IT devices are less safe. Operating system windows 7 is also in a case in point. Microsoft stopped supporting this system in 2020 but its still using by millions of peoples. Still, its running. Working from home also can open the door to the hackers. All the devices on the security risks. there can be a huge loss of confidential data. Thereby, leading to a spurt of cyber crime cases due to the coronavirus outbreak in India and worldwide.

One such application which was accessible in Google Play Store was "corona live 1.1", which professed to be a live tracker of instances of Coronavirus. Individuals utilizing the application were of the view that they are monitoring the pandemic, yet the vindictive application was really attacking their security: gaining admittance to the gadget's photographs, recordings, area and camera. The data gathered can be utilized multiplely, they can be utilized to bargain your financial balances or even coercion the proprietor of the photos and recordings. Now the apps are available on fake websites, one such being 'coronavirusapp.site', where the link to download the app is listed. These instances adequately demonstrate the rise in cyber crime on account of coronavirus.

Take the case of the new information break at the installment firm Mobikwik. It was accounted for that the information penetrate occurrence has influenced 3.5 million clients, uncovering know-your-client records like locations, telephone numbers, Aadhaar card, PAN cards, etc. The organization, till now, has kept up that there was no such information penetrate. It was solely after the controller Reserve Bank of India (RBI) requested that Mobikwik get the scientific review led quickly by a CERT-IN empanelled inspector and present the report, that the organization is working with imperative specialists. For clients in India if there should arise an occurrence of information penetrates they are in a fix as India doesn't have a particular enactment managing client information break cases or reformatory activities identifying with something similar. The Personal Data Protection Bill, which is proposed to manage such instances of information penetrates, has been forthcoming in the Lok Sabha since 2019.

PREVALENT CYBER CRIMES

Despite the fact that digital violations have been expanding consistently, there has been an upsurge during the lockdown because of individuals doing all the authority just as un-official work from their workstations or telephones. Other than programmers straightforwardly assaulting the frameworks, counterfeit sites are being made to trap the clients.

Human hacking known as “Social engineering” also manipulated the peoples. It consists sending email, text messages on social media platform with the malicious links to files which downloaded or forms.

Hacking at companies and offices Companies have set up a VPN structure, to let the employees have access to all the information, which has become the target of the hackers. Hackers are trying to hack the software of the companies in order to gain access to all their important details and data. There have been cases of unwanted software trying to infiltrate to the companies' systems for theft and malicious payloads. There have been several attempts made by the hackers at banks and Stock Markets leading to the brokerage. PM's COVID fund has also been one of the targets of the Hackers.

Spyware consists obtaining data which can be used or sold later . generally information of medically or financially in nature. Ransomware encrypted the victims devices with the unknown code . then criminal will demand a ransom for exchanging the code that will let the victim recover his device and data. Spy-attacks and Ransom attacks are posing a threat to people submitting personal information online. Spyware steals the personal information and account details of the users, whereas a ransom attacker dominates and takes over the login credentials of the user. An app called 'Covidlock' is used as ransomware to target the anxious population, misrepresenting the same as an app to keep track of the spread of coronavirus.

Phishing mail is the popular method. Phishing is the cybercrime where the criminal accesses the information and details of the user through a link or e-mail that seems legitimate but is in fact, fraudulent. Phishing and online scams are most common cyber crime technique . Phishing fraudulently practice of inducing individual to reveal personal information such as password and credit or debit card number through the email or fake websites. After the covid – 19 and imposing lockdown , has lead to more people to be confined at home increasing relying on the internet. New data from Google or VPN (Virtual private Network) service provide is growing very fast. In January , Google registered 149 active cases on phishing websites, In February 293k and in March 522k . During covid 19 Pandemic, cyber crime cases increasing whole over the world. In Italy, a Corona anti - virus software has also been flagged to the Italian enforcement authorities. Children are also exposed to threats which coming from the internet, file sharing misuse, inappropriate content , grooming of children for the sexual purpose are some example of dangers . So their parents should be aware of this challenging time.

Patients at risks - Increasing of cyber attacks on healthcare organizations and institutions so hospitals and other healthcare organizations are the become the target of ransomware. Criminals using malware to encrypt the stored data of the victims in order to blackmail them afterwards. Ransomware attacks have been detected in hospitals and other test centres where the important files of the patients are taken and not returned till a particular amount of ransom is paid.

Other online crimes related to social media : Social networking apps like Facebook, WhatsApp. YouTube, Google, Facebook, Twitter etc. have become an important tool to spread fake information. These fake news' triggers the people, as they blindly believe these reports, and start reacting accordingly. Besides this, these online chatting apps are misused to sexually harass people.

From the lockdown, various percentage of people connected with internet and spending time online.so it provided more opportunity for the cyber offender for earning more money and create disruption. From this lockdown, children are spending more time on internet for services such as schooling. Disruptive malware against the healthcare institutions by the cyber criminal for the financial benefits. In April 2020, there was ransomware attacks by the various threat group . The deployment of data harvesting malware such as spyware, banking Trojans, remote access Trojans , steal data by the cyber criminals are on rise.

Misinformation and fake news among the people is also spreading during this covid – 19.there are many reports linked to the illegal trade of fraudulently medical commodities, large discount in super market etc.

During covid pandemic, digital security risk on the working from homes to breach data.

Another demand is growing for pornography in this lockdown.

PROTECTION MEASUREMENTS

- Don't download and installed from unofficial website
- always avoid false information or fraudulent links
- Don't provide medical or financial information unless its via official channel which confirmed by the competent authority
- Confirm origin of communication which you received
- Always installed best security technology
- Protect your device with strong password
- Check the App details on Playstore before downloading it, this includes, details of the developer, their website (if any), reviews and ratings given by other users.
- Avoid downloading apps from third-party stores and websites, and download the apps only available in App Store for Apple IOs users and Google Playstore for Android users.
- Use reliable mobile and desktop antivirus, these can prevent fake and malicious apps from being installed.
- Do not believe any emails that come with a sense of panic. Legitimate organizations will never want you to panic and they always take the processes step by step.
- Do not believe that WHO or any other organization conducts lotteries or offer prizes, grants or certificates through emails.
- HTTP = Bad, HTTPS = Good: The 'S' in https:// stands for 'secure'. It indicates that the website uses encryption to transfer data, protecting it from hackers.
- Check for easy markers such as spelling mistakes, typos and broken links. It is highly improbable for a legitimate business to have such mistakes on their website.

CYBER LAWS IN INDIA

Information Technology Act, 2000 is the only specific actions we have which is the basis of cyber laws and provides for different cybercrimes, their punishment, and sufficient Remedies.

The ransomware attacks are punishable under Section 66 E and 66 F of the Information Technology Act, 2000. Under section 43 of the IT act, Hacking is a civil offense but if committed in a fraudulent way the person is punishable with imprisonment under section 66 B. The offense of phishing is punishable with imprisonment up to 3 years and a fine up to 1 lakh under Section 66 C of the IT Act. Section 72 and 66 of the IT Act provides for the crime of cyber-stalking and online harassment.

Besides IT Act, 2000, the Indian Penal Code, 1986 also provides with some of the punishments and remedies for cyber-crimes: Section 419 of IPC provides for the frauds by impersonation. Section 354 of IPC provides for the crime of cyber-stalking and online harassment and its punishment with imprisonment up to 2-3 years. The persons spreading fake news can be arrested under Section 505 of the IPC and Section 54 of Disaster Management Act, 2005 and can be punished with imprisonment up to 3 years and fine up to 1 lakh or both.

LACUNA IN EXISTING CYBER LAWS

The problem of cyber laws in India starts with not having any set definition of cyber-crime in any act or law. Though there are some laws and remedies in the IT Act, 2000 but there are a lot of grey areas. These include intellectual property rights including copyrights, infringement and trademark. Moreover, there are no specific inclusions or the scams against the big companies and hence have to be treated only under the sections of hacking and online fraud. No separate policies are enacted for handling the cybercrimes against the health care sectors.

Territorial Jurisdiction is another major issue which is not specifically dealt by any cyber law. Since cyber crimes are computer and internet-based crimes, the hacker is far-sitting and maybe in another state and hence determination of jurisdiction is difficult. Preservation of evidence is another problem. As most of the evidence and proofs are online and in systems, destruction of the evidence is easy.

Besides this, the already existing laws are limited only to the theoretical punishments as it is not easy to prosecute the criminal due to anonymity. There are no concrete measures to take actions against these online criminals and no strategy to find these criminals sitting far away in comfort away from the actual location.

CONCLUSION & SUGGESTIONS

Technology provided powerful tools but it must be used with the appropriate safety measurement. It should be noticed that how people using the technology. There is no 100 percent security on cyber domains. Cyber crime is using by the advent of digitalization. Now covid vaccine is available , but then also there is problem of phishing related to medical products and network incrustation and stealing data. The main target of criminals are among the public who now using most of time online and the employer who working from home. There is need to awareness of cyber security. For avoiding covid related crime, there is need to educate employees, ensure systems are robust, keep updated technology and automate manual processes. Criminals take advantages of human vulnerability to steal user data. It is sure that the security norms have decayed as numerous associations were not prepared to work distantly and an ascent has been observers in digital wrongdoing due to Covid. With a little watchfulness and due industriousness we can secure our information and protection. It is in every case better to remain in favour of precautionary measure yet in the event that, even subsequent to avoiding potential risk, we fall into a snare a speedy activity can rescue the misfortune. It is prudent to stop a grievance with the fitting position. Now rate of unemployment are also increasing meaning that more people are sitting at home online

The government must ensure the safety of the state digital network & systems which store important public information and must take concrete steps in this regard. The lockdown has exposed the weak cyber-laws and after about a 5 percent increase in cyber-crimes, the government has shifted some focus to this side and the cyber-centers and cyber-police have become active. The government is issuing an advisory to the public to not to fall prey to these only crimes and take precautions while filling their details and passwords on online sites. But the government also needs to come up with some stronger laws, procedures, and strategies to catch the hackers. Besides, there is a need to introduce some security applications to prevent the companies' systems and hospital computers from hacking.

These are some of the short-term solutions during the lockdown but there also needs some reform in the current Information Technology Act, 2000 as it is a comprehensive act and does not include much of the other aspects which are affected by the cyber-crimes.

REFERENCES

Cybersecurity Ventures, “2019 offi-cial annual cybercrime report,” 2019,https://www.herjavecgroup.com/the-2019-official-annual-cybercrime-report

www.atlasvpn.com/blog/google-registers-a-350-increase-in-phishing-websites-amid-quarantine/

www.globalinitiative.net/crime-contagion-impact-covid-crime/

www.mondaq.com

R. Smithers, “Fraudsters use bogus nhs

contact-tracing app in phishing scam,” 2020, https://www.theguardian.com/world/2020/may/13/

fraudsters-use-bogus-nhs-contact-tracing-a

R. Smithers, “Fraudsters use bogus nhs

contact-tracing app in phishing scam,” 2020,

https://www.theguardian.com/world/2020/may/13/

fraudsters-use-bogus-nhs-contact-tracing-a

R. Smithers, “Fraudsters use bogus nhs

contact-tracing app in phishing scam,” 2020,

https://www.theguardian.com/world/2020/may/13/

fraudsters-use-bogus-nhs-contact-tracing-a

MalwareBytes, “Cybercriminals impersonate WorldHealth Organization to distribute fake coronaviruse-book,” 2020, https://blog.malwarebytes.com/social-engineering/2020/03/cybercriminals-impersonate-world-health-organization-to-distribute-fake-coronavirus-e-book/

The Times, “Fraudsters impersonate airlinesand Tesco in coronavirus scams,” 2020,https://www.thetimes.co.uk/article/fraudsters-impersonate-airlines-and-tesco-in-coronavirus-scams-5wdwhxq7p, (Accessed

R. Smithers, “Fraudsters use bogus nhscontact-tracing app in phishing scam,” 2020,https://www.theguardian.com/world/2020/may/13/fraudsters-use-bogus-nhs-contact-tracing-app-in-phishing-scam

W. H. O. (WHO), “Who coronavirus disease (covid-19)

dashboard,” 2020, thttps://covid19.who.int/, (

W. H. O. (WHO), “Who coronavirus disease (covid-19) dashboard,” 2020, thttps://covid19.who.int

World Health Organisation (WHO), “Coron-avirus disease (COVID-19) pandemic,” 2020,https://www.who.int/zh/emergencies/diseases/novel-coronavirus-2019